Análise de Risco em Ambientes Corporativos na Área de Tecnologia da Informação

Laerte Peotta Paulo Gondim
Universidade de Brasília - UNB

RESUMO

Um tema que vem sendo muito discutido é a governança em TI (Tecnologia da informação), no entanto existem muitos métodos e técnicas de gestão que podem ser adotadas para se implementá-la. Um bom ponto de partida seria elaborar um plano para análise de risco em TI, controlando e conhecendo a infra-estrutura, agilizando a tomada de decisão visando reduzir ou mitigar o risco. Neste artigo será descrito uma metodologia para efetuar uma análise de risco eficiente.

Palavras-Chave: Gestão de risco, Segurança da informação, Governança, Compliance.

1. INTRODUÇÃO

A premissa básica para uma boa governança em TI é o fato de que deve se conhecer o ambiente interno para uma tomada de decisão acertada, pois o que não se conhece não pode ser gerenciado.

Em uma empresa a área de TI pode ser tratada apenas como commodities, mas essa decisão pode transformar o modo como a empresa opera, sendo pouco acertado em alguns casos tratar a TI como não sendo área fim do negócio. A situação se agrava, pois muitas empresas mantêm negócios na internet e mesmo assim a área de TI fica terceirizada, podendo incorrer diversos riscos que acabam indo além das previsões da empresa e seus controles.

Atualmente as empresas estão bastante preocupadas com o tema segurança da informação, no entanto é necessário encontrar um método que avalie constantemente os ativos internos, auxiliando não somente a análise de risco, mas toda a gestão de TI, pois o conhecimento da infra-estrutura e dos ativos gera conseqüente reflexo na gestão.

A visão de um analista de risco em TI é poder identificar uma vulnerabilidade, calcular um score sobre a vulnerabilidade, verificar se essa falha afeta o negócio da empresa e por fim atuar de maneira a corrigir o problema, devendo o trabalho ser efetuado no menor tempo possível.

Aparentemente o trabalho é simples, pois são poucos passos a seguir, no entanto a quantidades de vulnerabilidades divulgadas vem crescendo exponencialmente, tornando o trabalho cada vez mais complexo a ponto de não ser mais possível controla-lo de maneira manual ou mesmo semi-automatizado.

Outro aspecto relevante na análise de risco que deve ser observado é a necessidade cada vez mais exigida pelo mercado: a transparência das informações. Isso pode ser confirmado com o número crescente de exigências pelos órgãos reguladores que vem literalmente obrigando a cumprir normas como:

- Sarbanes- Oxley (SOX) [Lahti (2005)];
- Acordos de Basiléia I e II [Saidenberg (2003)];

- ISO 17799 [ABNT (2005)], ISO 27001[ISO/IEC (2005)] ou a BS-7799 [BSI (2001)] para a gestão de segurança da informação.

A adequação a esses padrões internacionais pode gerar custos extras, e em alguns casos, inclusive perda de competitividade, mas isso geralmente é considerado em curto prazo. Quando se avalia a adoção desses padrões e seus resultados a médio/longo prazo pode se ter claramente uma visão positiva, demonstrando uma maturidade e preparo que podem, inclusive, atrair novos investimentos e gerar um sentimento elevado de segurança aos acionistas.

O risco pode ser definido como a probabilidade de que uma situação física com potencial de causar danos possa ocorrer, em qualquer nível, em decorrência da exposição durante um determinado espaço de tempo a uma vulnerabilidade, que por sua vez é definida como uma fraqueza em um sistema, que pode envolver pessoas, processos ou tecnologia que pode ser explorada para se obter acesso a informações.

Na existência de uma vulnerabilidade tem-se um risco que decorre do surgimento de uma ameaça que definimos como qualquer circunstância ou evento com o potencial de causar impacto sobre a confidencialidade, integridade ou disponibilidade da informação. Por este motivo a classificação da informação se torna um dos itens mais importantes do ciclo no processo da segurança.

Algumas ferramentas ou mesmo metodologias, tentam explorar as vulnerabilidades diretamente [agris 2004], o que pode levar a perda de informações, comprometimento dos serviços e muitas vezes a sobrecarga da própria rede. Em alguns casos as informações coletadas podem não espelhar a realidade, pois podem existir inconsistências na obtenção dos dados.

A análise de risco pode ser mais complexa que outros temas, mas tudo depende de um bom planejamento e conhecimento prévio do ambiente tecnológico que será aplicado à análise, para tanto definimos como sendo um processo que visa identificar, analisar, reduzir ou transferir o risco [Stoneburner (2002)].

2. TRABALHOS RELACIONADOS

Na proposta de elaboração deste artigo não encontramos nenhum trabalho que se propusesse a executar uma análise de risco de ativos da informação e que retornasse as condições atuais em tempo real, ou seja, no momento que uma vulnerabilidade é encontrada e reportada. Neste contexto os trabalhos que contribuíram para o atingimento do foco inicial descrevemos aqui.

Em [Perera (2005)] são colocadas as informações necessárias para se definir termos sobre risco e segurança. Também é sugerida uma matriz para análise de risco, orientando a elaboração de um *framework* conforme a figura 1.

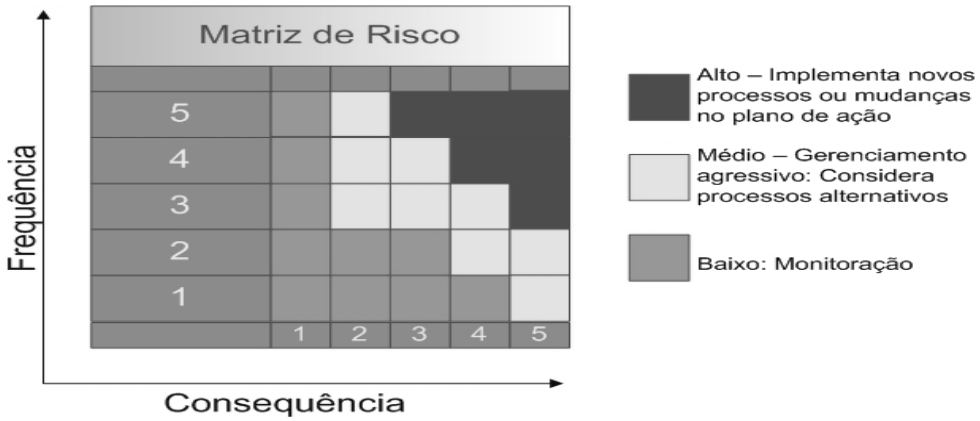

Figura 1: Matriz para avaliação de risco [Perera (2005)]

Os autores propuseram a criação de um sistema de gestão de risco pela IRMA (Intergovernmental Risk Management Agency). O ponto negativo desta ferramenta é que o risco é colocado sempre de forma manual, ou seja, deve existir a figura de um analista de risco para impostação das informações.

Em [Fussell (2005)] os autores colocam métodos para gestão da informação, descrevendo os processos que envolvem o tema e que tendem para a gerência de risco. O ponto negativo deste trabalho é também o mesmo que o trabalho [Perera (2005)], a falta de um agente que automatize de forma sistêmica a coleta de informações da rede que se pretenda implementar o método para gestão de risco.

Em [Dorofee (2001)], é apresentado um método chamado OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), onde uma equipe, chamada de equipe de análise, gerencia o processo e analisa toda a informação. Organizando ações diretas, tomando decisões de acordo com a situação.

O método tem três fases distintas:

1. Construção de um perfil de ameaça: onde se deve conhecer a estrutura da rede e organização das informações;
2. Identificação de vulnerabilidades: Nesta fase deve-se avaliar a infra-estrutura e levantar pontos de vulnerabilidades;
3. Desenvolvimento de estratégia e plano de segurança: Esta fase pode ser considerada a mais importante, é onde será desenvolvido um plano de ação para a análise de risco.

O ponto que torna o método difícil de aplicar é a necessidade de uma equipe exclusiva para a análise de informações/risco e conseqüente tomada de decisão.

3. COMMON VULNERABILITY SCORING SYSTEM

Vários órgãos e departamentos ligados a segurança da informação como o NIST (National Institute of Standards and Technology), FIRST (Forum of Incident Response and Security Teams), CERT (Computer Emergency Response Team) entre outros, se juntaram para criar um padrão para pontuação/mensuração de vulnerabilidades de software chamado de CVSS [Schiffman (2005)].

Historicamente, a indústria tem utilizado diversos métodos de scoring para vulnerabilidades de softwares [Mell (2006)], geralmente sem detalhamento desses critérios ou processos, criando um grande problema para os usuários, que precisam encontrar um meio de gerenciar seus sistemas e aplicações.

É importante saber que toda vulnerabilidade tem um tempo de vida [Frei (2006)], e que deve ser respeitado e seguido para a solução do problema.

O NIAC (National Infrastructure Advisory Council) escolheu o FIRST para liderar o projeto e avaliar um padrão aberto e universal onde deverá ajudar organizações a priorizar a segurança e análise de vulnerabilidades, consolidarem esforços do mundo todo e equipes de segurança para resolver o problema permitindo uma resposta mais rápida a riscos provenientes de vulnerabilidades conhecidas.

Para se calcular o score para uma determinada vulnerabilidade o CVSS tem como base três métricas principais:

- Métricas básicas (*Base Metrics*) contêm os atributos que são intrínsecos a toda vulnerabilidade.
- Métricas temporais (*Temporal Metrics*) contêm as características que evoluem de acordo com o ciclo de vida da vulnerabilidade.
- Métricas ambientais (*Environmental Metrics*) representam aquelas características únicas de acordo com o ambiente corporativo de onde está sendo implantada.

3.1 MÉTRICAS BÁSICAS

As métricas básicas são impostadas pelo fabricante, são compostas de acordo com a funcionalidade e utilização implícita em cada software, podendo ser adaptada com critérios. São definidos sete impactos para se obter um score que em conjunto com as métricas temporais e ambientais comporão o risco final:

- Dificuldade para acesso: mede a complexidade requerida para que um atacante consiga explorar o sistema alvo
- Vetor de acesso: indica se uma vulnerabilidade é explorada localmente ou remotamente
- Autenticação: indica se um atacante necessita ou não ser autenticado no sistema para conseguir explorar a vulnerabilidade
- Impacto confidencialidade: mede o impacto na confidencialidade (nenhum / parcial / completo)
- Impacto Integridade: indica o impacto na integridade
- Impacto Disponibilidade: impacto na disponibilidade
- Impacto CIA (Confidencialidade, Integridade, Disponibilidade): permite atribuir maior impacto em um dos pilares da CIA sobre os demais.

3.2 MÉTRICAS TEMPORAIS

As métricas temporais são determinadas de acordo com o tempo de vida de uma vulnerabilidade.

- *Exploitability*: indica se é possível ou não explorar a vulnerabilidade, podendo ser:
  - *Unproven:* (não há um exploit conhecido);
  - *Proof of Concept:* (foi criada uma prova de conceito indicando que a ameaça existe);
  - *Functiona:* (quando um exploit está disponibilizado);
  - *High:* (quando a vulnerabilidade está sendo explorada por um código malicioso ou mesmo manualmente).
- *Remediation Level*: informa se há uma solução conhecida:
  - *Official Fix*: quando o fabricante disponibilizou uma correção/patch;
  - *Temporary Fix*: (fornecida uma correção temporária pelo fabricante);
  - Workaround e Unavailable: Trabalhando e indisponível.
- *Report Confidence*: Representa o grau de confiança na existência da vulnerabilidade e na credibilidade de sua divulgação *(Unconfirmed / Uncorroborated / Confirmed)*.

3.3 ENVIRONMENTAL METRICS

São as únicas que são definidas de acordo com a realidade de cada empresa e, portanto podem ser manipuladas pelos gestores, consultores e auditores para representar a realidade em sua corporação:

- *Collateral Damage Potential*: mede o potencial de dano, podendo representar o risco de perda do equipamento físico, os danos de propriedade.

- *Target Distribution*: indica o tamanho relativo da quantidade de sistemas que são suscetíveis à vulnerabilidade (Nenhum; Baixo até 15%; Médio até 49% ou Alto - se acima de 50% dos sistemas são vulneráveis).

4. O PROCESSO DE SCORING

O processo de Scoring irá definir o valor final resultante da aplicação de todas as métricas, combinando todos os valores de acordo com fórmulas específicas conforme [Schiffman (2005)].

Da combinação dos três grupos descritos no projeto CVSS obtêm-se o score final.

Todo este sistema de métricas pode ser representado sinteticamente através de vetores conforme tabela 1.

Tabela 1: CVSS - Definição dos vetores [Schiffman (2005)]

Vetor	*Descrição*
Vetor básico	*AV:[R,L]/AC:[H,L]/Au:[R,NR]/C:[N,P,C]/I:[N,P,C]\\ & /A:[N,P,C]/B:[N,C,I,A]*
Vetor temporal	*/E:[U,P,F,H]/RL:[O,T,W,U]/RC:[N,U,C]*
Vetor de ambiente	*/CD[N,L,LM,MH,H]:/TD:[N,L,M,H]*

Desta maneira existe certa facilidade na impostação dos dados ou mesmo no seu tratamento por parte de um programa gerenciador.

5. COMMON VULNERABILITIES AND EXPOSURES (CVE)

Define-se como um padrão no tratamento e divulgação de informações sobre vulnerabilidades reportadas. O CVE (Common Vulnerabilities and Exposures) é um banco de dados público em que todos interessados possam obter acesso a informações sobre vulnerabilidades.

O conteúdo do banco de dados CVE é resultado de esforços colaborativos entre várias entidades ligadas a segurança da informação, entre elas: Sans Institute, Cancert, CERT, entre outras.

O principal gestor do CVE é o MITRE (Massachusetts Institute of Technology's Digital Computer Laboratory). Como o projeto é colaborativo, não é exigida uma contribuição, mas pode ser feita, tanto financeiramente quanto em relação à divulgação de informações.

A proposta geral do MITRE com a utilização do CVE não é apenas a divulgação de informações sobre o aspecto de vulnerabilidades e segurança, mas principalmente a padronização de como essa informação deve ser encaminhada e tratada. Dessa forma corrigem-se eventuais duplicações de informação e trata de maneira eficiente os dados coletados, permitindo uma maior compreensão e consequentemente qualidade na obtenção de dados relacionados à segurança.

6. GESTÃO DE ATIVOS

Segundo a norma ABNT NBR ISO/IEV 17799 de 2005, o item gestão de ativos foca a responsabilidade pelos mesmos, ou seja, todos os ativos da empresa devem ser identificados e atribuído uma responsabilidade sobre a sua manutenção baseada em controles.

É conveniente que os ativos identificados sejam documentados e a eles atribuído uma importância. Também se deve considerar a importância sobre o ativo, caso este seja comprometido.

Para uma eficiência em uma análise de risco deve-se partir do principio de que se conhece toda a infra-estrutura tecnologia [Chew (2006)]. Existem diversas maneiras conhecidas para se obter essa informação:

- Através de pesquisas manuais de descoberta na rede;
- Utilizando-se de entrevistas com responsáveis diretos pela infra-estrutura;
- Visitando todos os pontos de conexão
- Catalogando por inventário todos os componentes da rede.

O processo de gestão de risco é continuo e deve ser sempre reavaliado em busca de inconsistências. Podemos dividir o processo de condução de uma análise de risco em seis partes (figura 2):

- Planejamento e estratégia: planejar ações e criar estratégias de avaliação
- Identificação: Criar procedimentos para uma correta identificação dos riscos;
- Qualificação: Introduzir uma qualificação decorrente de uma vulnerabilidade;
- Quantificação: Possibilitar uma pontuação do nível de risco;
- Impactos e respostas: Criar procedimentos para se determinar o impacto sujeito e qual resposta deverá ser utilizada;
- Monitoramento e Controle: Determinar procedimentos para um constante acompanhamento para ações.

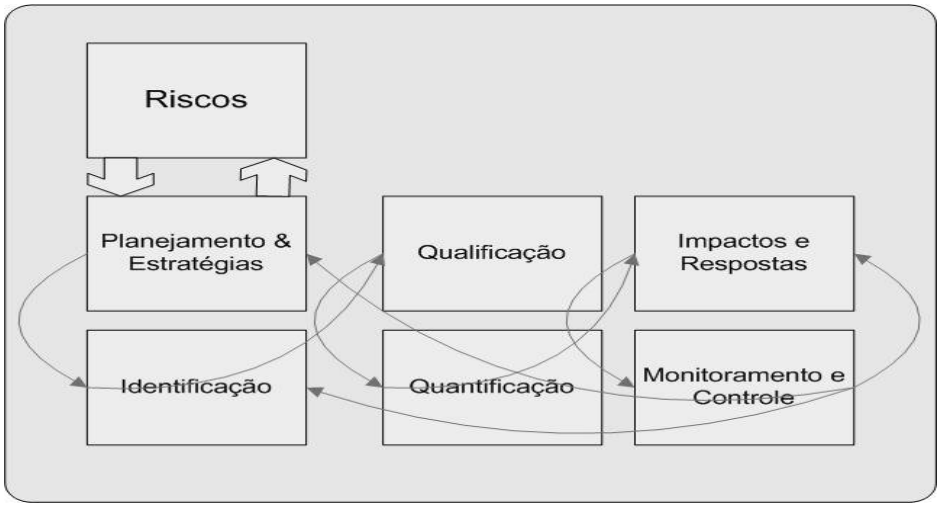

Figura 2: Processos Gestão de Riscos [scudere 2006]

Nos pontos aqui descritos, pode-se ter uma idéia que em redes de pequeno/médio porte (até 1000 máquinas) seria viável efetuar um dos itens acima. Infelizmente no momento que terminar de se coletar a ultima informação e consequentemente iniciar o processo de scoring de risco, toda a análise estará baseado no passado, ou seja, a análise de risco não terá a mesma eficiência, e a cada minuto que se passa menos eficiente estará. Com isso pode ocorrer uma falsa sensação de segurança.

6.1 PROCEDIMENTOS DE INVENTÁRIO

A velocidade na coleta da informação e sua constante atualização decorrido das mudanças que ocorrem a todo instante é a chave de sucesso para uma análise de risco eficaz.

Desta maneira é proposta uma ferramenta que deve atender aos seguintes requisitos:

- Possuir suporte característico cliente/servidor;

- Ter um banco de dados central, onde todas as informações serão armazenadas;
- Ser multi plataforma, de modo a rodar em diversos sistemas;
- Ser gerenciável para que se possam solicitar informações a qualquer momento que se faça necessário;
- Consumir o mínimo de recursos necessários para o funcionamento do cliente;
- Ser capaz de informar caso o cliente por algum motivo seja desabilitado;
- Poder ser reconfigurado a qualquer instante, de forma global, independente da vontade do usuário.

Desses requisitos iniciais, a ferramenta também deverá ser capaz de coletar diversas informações de inventário, sendo toda a informação enviada diretamente ao banco de dados central. Informações essenciais:

- Versão do sistema operacional corrente;
- Correções aplicadas e suas respectivas versões;
- Informações de usuários cadastrados e logados;
- Lista de softwares instalados e suas versões;
- Checagem de instalação de sistemas antivírus e suas atualizações;
- Informações sobre compartilhamentos;
- Informações de localização física do hardware (neste caso a informação deverá ser solicitada ao usuário);
- Lista de hardwares.

Após a coleta das informações para a geração de uma base de conhecimento da infra-estrutura de TI deve se proceder à qualificação quanto à importância do ativo. Para tanto um pequeno questionário pode ser adotado considerando cinco itens:

1. Irrelevante
2. Relevante
3. Importante
4. Crítico
5. Vital

7. PROPOSTA DE FRAMEWORK

A proposta deste artigo é a criação de uma metodologia para coleta, tratamento e apresentação de dados sobre vulnerabilidades, correlacionando os eventos com informações obtidas em uma rede interna.

Foi criado um diagrama de caso de uso contendo duas visões: A visão por parte do gestor (figura 3), e a visão por parte do usuário (figura 4).

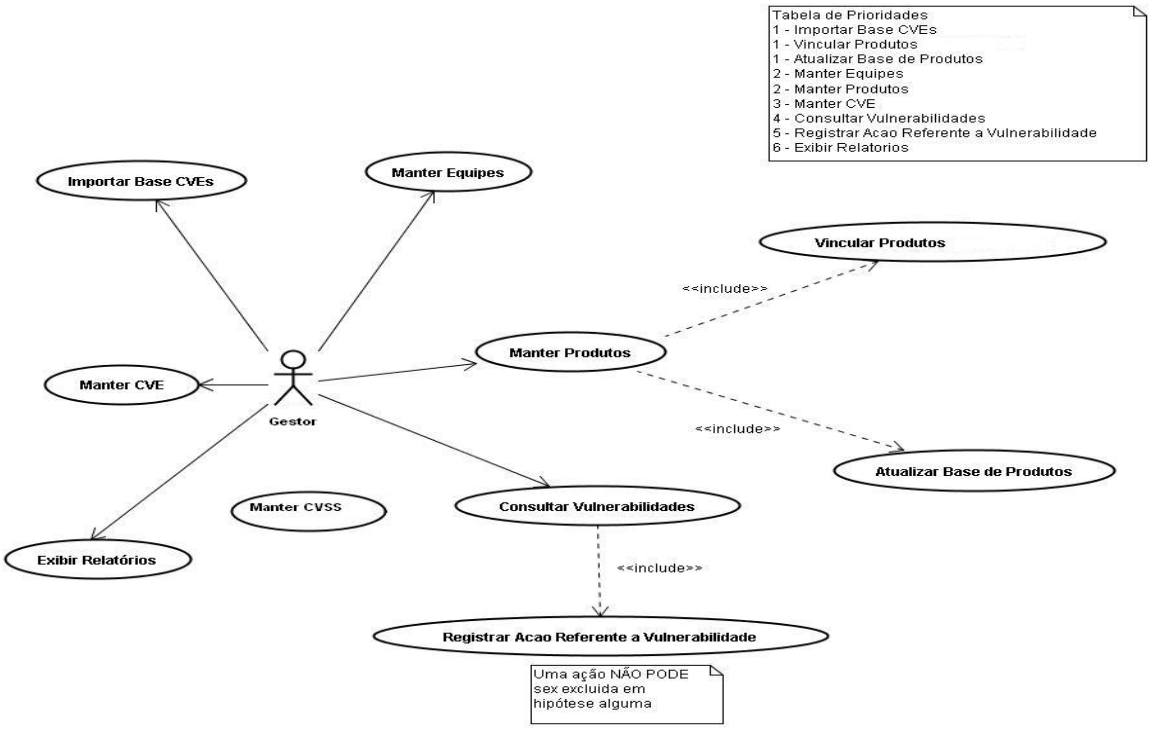

Figura 3: Diagrama de caso de uso – Gestor

Não é possível que o usuário veja ou acesse a visão do gestor, no entanto o gestor tem a visão total do sistema. A idéia é ter várias equipes vinculadas com visões diferentes para cada usuário.

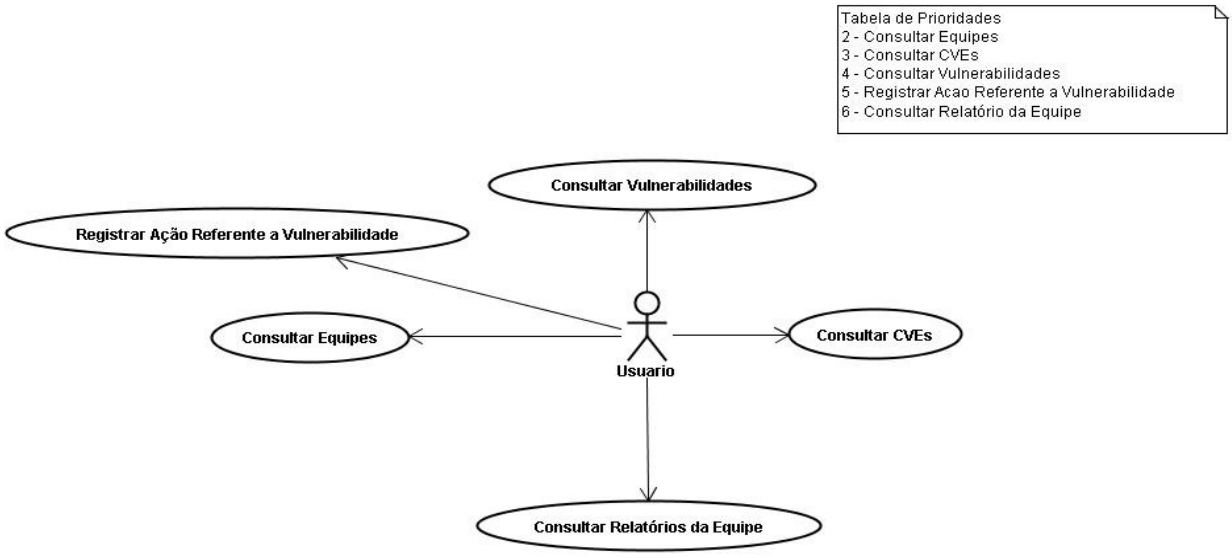

Figura 4: Diagrama de caso de uso – Usuário

As bases de dados CVSS e CVE descritas neste artigo servirão para popular um banco de dados interno, gerando uma base de vulnerabilidades chamada aqui de Risco, essas informações serão cruzadas com os dados de software e hardware coletados em uma rede interna, gerando a base com o conteúdo:

- IP (Internet Protocol) da máquina na rede;

- Versão de softwares instalados;
- Informações sobre usuários logados no domínio;
- Tipo do sistema operacional;
- Informações sobre hardware (memória, processador, Hard disk).

A base de dados gerada através da coleta de informações internas será denominada inventário.

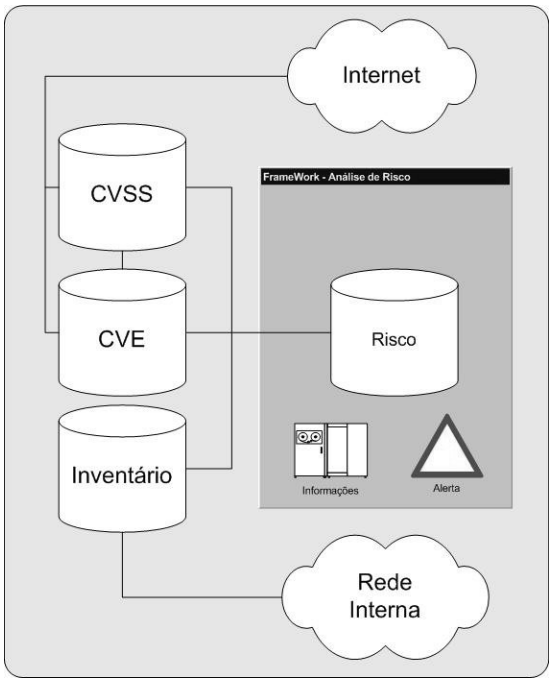

Figura 5: Modelagem de infra-estrutura de risco

Conforme a figura 5 o diagrama demonstra a interligação/correlação das informações, sendo que a base CVSS e CVS é alimentada por organizações externas. A base Inventário e Risco são mantidos pela entidade interna. Para que o procedimento seja eficiente todas as máquinas do domínio deverão ter instalado o software de inventário que irá alimentar a base interna. Neste caso deverá constar, caso exista, na política de segurança da empresa, caso não exista uma política consolidada deverá pelo menos ser criada uma norma de conduta e utilização dos ativos por parte dos usuários.

A princípio a norma deverá conter informações sobre:

- Instalação e utilização de software não homologado pela instituição, de modo que impeça o usuário a instalar qualquer sistema que não conste no catalogo interno, com isso evitando instalações até mesmo de software sem licença;
- Termo de responsabilidade de utilização dos ativos tecnológicos, explicitando sua utilização apenas para fins diretos do negócio;
- Metodologia para utilização de ativos móveis (notebooks, PDA`s, etc.) sendo vetada a utilização de equipamentos externos, ou seja, que não faça parte dos ativos próprios;
- Criação de métodos para instalação de novos ativos, sendo que qualquer equipamento ligado na rede deverá ter em seu enxoval de instalação o software de inventário.

- Criação de procedimentos de logins de usuários na rede, protegendo contra conexões espúrias, de modo que apenas ativos com o software de inventário serão permitidos no ambiente local;
- Por fim uma política de divulgação do projeto de modo que o maior número de pessoas possa conhecer e consequentemente apoiar.

7.1 ADEQUAÇÃO DO SCORE RISK

Com todas as informações coletadas deve-se rever a pontuação gerada automaticamente e verificar através de um questionário a avaliação de servidores considerados críticos, dessa maneira terá informações sobre quais máquinas/servidores tem maior impacto caso esta seja comprometida tanto por problemas físicos quanto lógico. Foi criado um fluxo (figura 6), onde é descrito os passos necessários para a coleta e calculo do risco.

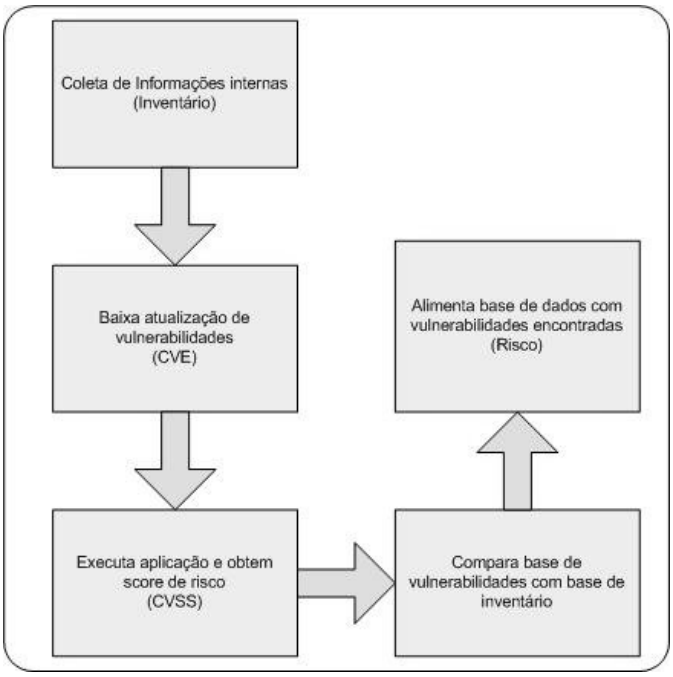

Figura 6: Procedimentos de coleta de informações

O Framework poderá auxiliar com as seguintes informações:

- Determinar o valor dos ativos de informação bem com sua criticidade para a corporação;
- Estimar uma determinada probabilidade de uma ameaça poder ocorrer e possibilitar o calculo do custo;
- Identificar pontos vulneráveis e subsidiar decisões para contornar ou diminuir o risco;
- Permitir a criação de estratégia para mitigar os riscos;
- Possibilitar a correta identificação dos ativos.

8. CONCLUSÕES E TRABALHOS FUTUROS

As leis de vários países estão sendo adaptadas visando dar maior transparência às operações das empresas. Com essa clareza os investidores poderão fazer seus investimentos com maior segurança. Por parte da empresa ocorrerá ganhos relacionados à qualidade de seus processos, tornando-a mais competitiva e, conseqüentemente, podendo aumentar seus ganhos financeiros.

Nos últimos anos foram investidos valores consideráveis para obtenção de equipamentos e soluções de segurança, como sistemas de detecção de intrusos, antivírus, firewalls, anti-spam, e uma infinidade de outras soluções. Mas como realmente saber se esses investimentos tiveram o retorno esperado? As informações geradas muitas vezes são ignoradas, ou quando tratadas pouco auxiliam na gestão da informação. É nesse ponto que a gestão de risco vem ao auxilio, consolidando os dados coletados e transformando em informações utilizáveis.

O framework proposto neste artigo depende de vários fatores, o principal é a aceitação da idéia por parte dos gestores de que o investimento em segurança da informação é algo que lhes trará retorno, e no mundo corporativo o retorno tem que ser de caráter financeiro.

Outro fator relevante é de que se conhecerá a infra-estrutura geral de TI, podendo mensurar os investimentos e retorno (ROI), com isso elaborar um plano de ação para o tratamento e análise de risco, visando a conseqüente mitigação dos riscos.

A ferramenta aqui proposta deverá, a principio, ser de caráter informativo, subsidiando o gestor de informações sobre sua própria base, aplicando-se regras fundamentais da arte da guerra[1].

- Se conheceres a si próprio terás chances de vitória;
- Se conheceres a si próprio e a seu inimigo terás a vitória;
- Se não conheceres nem a si e nem o seu inimigo a derrota serás certa.

Esta metáfora é devido a constante guerra que está sendo travada na rede mundial de computadores, onde empresas desonestas podem querer obter informações de maneira ilícita para que assim tenham vantagens sobre suas concorrentes. Conseqüentemente o *inimigo* é qualquer pessoa/empresa que se utilize de conhecimentos e informações obtidos de maneira não legal e os utilize para si, podendo gerar prejuízos para seus concorrentes.

O fato é que não é possível um gerenciamento eficiente de risco se não for possível identifica-lo, pois o risco ocorre tendo como premissa a incerteza, caso não exista incerteza não existe risco. É neste contexto que o trabalho está sendo desenvolvido, visando reduzir as variáveis de incerteza concomitantemente reduzindo o risco.

Em trabalhos futuros pretende-se desenvolver uma metodologia ativa em relação às vulnerabilidades, tornando-as inócuas à medida que forem detectadas, de maneira totalmente automatizada e transparente para o usuário.

O framework deverá permitir que vulnerabilidades sejam localizadas e corrigidas, identificando aspectos inclusive de comportamento do usuário.

9. REFERÊNCIAS

ABNT (2005). NORMA BRASILEIRA ABNT NBR ISO/IEC 17799:2005-Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. ABNT, Rio de Janeiro – RJ, segunda edição.

Alberts, C. e Dorofee, A. (2001). An introduction to the octave method.

(BSI), B. S. I. (2001). BS 7799:2001 - Information Security Management – Specification With Guidance for Use.

Chew, E., Clay, A., Hash, J., Bartol, N., and Brown, A. (2006) Guide for developing performance metrics for information security recommendations of the national institute of standards and technology.

[1] Sun Tzu

Christian Lahti, Steve Lanza, R. P. (2005). Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools. ISBN-10: 1-59749-036-9, ISBN-13: 978-1-59-749036-8. Syngress.

Frei, S., May, M., Fiedler, U., and Plattner, B. (2006). Large-scale vulnerability analysis. In LSAD '06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, pages 131–138, NewYork, NY, USA. ACM Press.

Fussell, L. and Field, S. (2005). The role of the risk management database in the risk management process. Pages 364–369.

ISO/IEC (2005). ISO/IEC 27001:2005 – Information Security Management-Specification With Guidance for Use. ISO

Mell, P., Scarfone, K., and Romanosky, S. (2006). Common vulnerability scoring system. IEEE Security and Privacy, 4(6):85–89.

Perera, J. and Holsomback, J. (2005). An integrated risk management tool and process. Aerospace 2005, IEEE Conference, (ISBN: 0-7803-8870-4, INSPEC Accession Number: 8939524, Digital Object identifier: 10.1109/AERO.2005.1559306):129–136.

Saidenberg, M., Schuermann, T., and May (2003). The new basel capital accord and

Questions for research. Technical report.

Schiffman, M. (2005). A complete guide to the common vulnerability scoring system (cvss). http://www.first.org/cvss/cvss-guide.html.

Scudere, L. (2006). Risco Digital. ISBN: 8535221913. Editora Elsivier, Rio de Janeiro.

Stoneburner, G., Goguen, A., and Feringa, A. (July2002). Risk management guide for information technology systems – recommendations of the national institute of standards and technology.

Carmo, Luiz Fernando. Costa, Ricardo de Barros e Reis, Carlos Augusto. Alves, Gustavo Alberto de Oliveira. Nascimento , Tiago Monteiro. (2004) . Estratégias De Mitigação De Riscos De Segurança Do Ambiente AGRIS - Núcleo de Computação Eletrônica Universidade Federal do Rio de Janeiro, Brasil